CLAIMS

We claim:

5   1.   A privacy protection system including a user side device (22) provided with a true user profile which comprises user related profile data, a profile generator (24) operable to generate at least one false user profile (26a-26c) which includes profile data not the same as the user's profile data, transmission means operable to transmit the at least one false user profile to a third party (14-18) with a data request, a receiving unit (28a-28c)

10   operable to receive a response from the third party generated on the basis of the false user profile, and a response analyser (30) operable to determine from the received response a response related to the true user profile.

     2.   A system according to claim 1, wherein the profile generator (24) is

15   operable:

        a) to generate a plurality of user profiles of which only one is a true user profile, or

        b) to generate a plurality of user profiles none of which includes a true user profile, or

        c) to split user data forming the true user profile into separate parts with the

20   separate parts being included in false user profiles to which are added false user data, or

        d) to generate entirely false profiles none of which contains any true user data.

     3.   A system according to claim 1, wherein the profile generator is operable to generate a plurality of false user profiles which provide a spread of user data enabling

25   interpolation of the received responses.

     4.   A system according to claim 3, wherein the false user profiles are generated on a random basis.

5.   A system according to any preceding claim, wherein the response analyser is operable to extrapolate or interpolate from the received responses in order to generate an estimated response for the true user profile.

5

6.   A system according to any preceding claim, wherein the system is operable to receive responses over a period of time.

7.   A system according to any preceding claim, wherein the user profile generator is provided in a user's communication device or is provided at a location remote

10   from the user.

8.   A privacy protection method including the steps of providing at a user side a true user profile (22) comprising user related profile data, providing a profile generator (24) which generates at least one false user profile (26a-26c) which includes profile data

15   not the same as the true user profile data, transmitting (42) the at least one false user profile to a third party (14-18) with a data request, receiving (44) a response (28c-28c) from the third party generated on the basis of the false user profile, and providing a response analyser (30) which analyses the response to determine from the received response a response related to the true user profile.

20

9.   A method according to claim 8, wherein:
a) a plurality of user profiles is generated of which only one is a true user profile, or
b) a plurality of user profiles is generated none of which includes a true user profile, or

25   c) entirely false profiles are generated none of which contains true user data, or
d) a plurality of false user profiles are generated which provide a spread of user data enabling interpolation of the received responses.

10.   A computer including a privacy protection system according to any one of

30   claims 1 to 7.

11.   A computer according to claim 10, wherein the computer is a personal computer, a portable computer, a hand held computer, a personal digital assistant or a mobile telephone.